



PERLINDUNGAN HUKUM TINDAK PIDANA CYBERCRIME DALAM CYBERLAW DI INDONESIA:

Perkembangan Teknologi dan Tantangan Hukum Dalam Mewujudkan Cybersecurity

Seri Mughni Sulubara, S.H., M.H
Viridya Tasril, S.Kom., M.Kom
Nurkhalisah



PERLINDUNGAN HUKUM TINDAK PIDANA CYBERCRIME
DALAM CYBERLAW DI INDONESIA: PERKEMBANGAN
TEKHNOLOGI DAN TANTANGAN HUKUM DALAM
MEWUJUDKAN CYBERSECURITY

Seri Mughni Sulubara, S.H., M.H
Virdyra Tasril, S.Kom., M.Kom
Nurkhalisah



Tahta Media Group

UU No 28 tahun 2014 tentang Hak Cipta

Fungsi dan sifat hak cipta Pasal 4

Hak Cipta sebagaimana dimaksud dalam Pasal 3 huruf a merupakan hak eksklusif yang terdiri atas hak moral dan hak ekonomi.

Pembatasan Pelindungan Pasal 26

Ketentuan sebagaimana dimaksud dalam Pasal 23, Pasal 24, dan Pasal 25 tidak berlaku terhadap:

- i. penggunaan kutipan singkat Ciptaan dan/atau produk Hak Terkait untuk pelaporan peristiwa aktual yang ditujukan hanya untuk keperluan penyediaan informasi aktual;
- ii. Penggandaan Ciptaan dan/atau produk Hak Terkait hanya untuk kepentingan penelitian ilmu pengetahuan;
- iii. Penggandaan Ciptaan dan/atau produk Hak Terkait hanya untuk keperluan pengajaran, kecuali pertunjukan dan Fonogram yang telah dilakukan Pengumuman sebagai bahan ajar; dan
- iv. penggunaan untuk kepentingan pendidikan dan pengembangan ilmu pengetahuan yang memungkinkan suatu Ciptaan dan/atau produk Hak Terkait dapat digunakan tanpa izin Pelaku Pertunjukan, Produser Fonogram, atau Lembaga Penyiaran.

Sanksi Pelanggaran Pasal 113

1. Setiap Orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf i untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp100.000.000 (seratus juta rupiah).
2. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah).

**PERLINDUNGAN HUKUM TINDAK PIDANA CYBERCRIME DALAM CYBERLAW DI
INDONESIA: PERKEMBANGAN TEKNOLOGI DAN TANTANGAN HUKUM DALAM
MEWUJUDKAN CYBERSECURITY**

Penulis:

Seri Mughni Sulubara, S.H., M.H
Viridya Tasril, S.Kom., M.Kom
Nurkhalisah

Desain Cover:

Tahta Media

Editor:

Proofreader:

Tahta Media

Ukuran:

vii, 109, Uk: 15,5 x 23 cm

ISBN : 978-623-147-938-9

Cetakan Pertama:

Juli 2025

Hak Cipta 2025, Pada Penulis

Isi diluar tanggung jawab percetakan

Copyright © 2025 by Tahta Media Group

All Right Reserved

Hak cipta dilindungi undang-undang

Dilarang keras menerjemahkan, memfotokopi, atau
memperbanyak sebagian atau seluruh isi buku ini
tanpa izin tertulis dari Penerbit.

PENERBIT TAHTA MEDIA GROUP
(Grup Penerbitan CV TAHTA MEDIA GROUP)
Anggota IKAPI (216/JTE/2021)

KATA PENGANTAR

Puji dan syukur kita panjatkan ke hadirat Allah SWT atas rahmat dan karunia-Nya sehingga buku berjudul *“Perlindungan Hukum Tindak Pidana Cybercrime dalam Cyberlaw di Indonesia: Perkembangan Teknologi dan Tantangan Hukum dalam Mewujudkan Cybersecurity”* dapat hadir sebagai salah satu karya ilmiah yang membahas secara komprehensif mengenai aspek hukum dari tindak pidana siber di era digital saat ini.

Perkembangan teknologi informasi dan komunikasi yang begitu pesat telah membawa perubahan besar di berbagai sektor kehidupan, termasuk perekonomian, sosial, pendidikan, dan pemerintahan. Namun, di balik kemudahan dan manfaat teknologi tersebut, muncul pula berbagai risiko dan ancaman baru berupa tindak pidana siber (cybercrime) yang berpotensi merugikan individu, institusi, bahkan negara secara keseluruhan. Oleh karena itu, perlindungan hukum yang efektif terhadap tindak pidana ini menjadi sangat urgent dan membutuhkan kajian mendalam, khususnya dalam konteks hukum Indonesia yang terus berkembang seiring dinamika dan tantangan dunia digital.

Buku ini disusun dengan tujuan memberikan pemahaman yang mendalam tentang aspek cyberlaw, termasuk analisis regulasi yang berlaku di Indonesia seperti UU Informasi dan Transaksi Elektronik (UU ITE), UU Perlindungan Data Pribadi, dan ketentuan lain yang mendukung penegakan hukum terhadap cybercrime. Selain itu, buku ini juga mengangkat berbagai permasalahan dan tantangan nyata dalam penerapan hukum siber, serta strategi strategis yang dapat diterapkan untuk mewujudkan cybersecurity yang holistik di Indonesia.

Saya berharap karya ini dapat menjadi referensi penting bagi akademisi, praktisi hukum, penegak hukum, pembuat kebijakan, maupun masyarakat luas yang ingin memahami lebih dalam mengenai perlindungan hukum terhadap cybercrime serta kontribusinya dalam menjaga keamanan dan kepercayaan di dunia maya.

Akhir kata, saya mengucapkan terima kasih kepada semua pihak yang telah memberikan dukungan dan kontribusi dalam proses penyusunan buku ini. Semoga buku ini dapat memberikan manfaat serta mendorong pengembangan hukum siber yang semakin kuat dan adaptif di Indonesia.

Medan, 05 Juli 2025 Penulis

Seri Mughni Sulubara, S.H., M.H

DAFTAR ISI

KATA PENGANTAR.....	iv
DAFTAR ISI	vi
BAB I PENDAHULUAN	1
A. Definisi Dan Ruang Lingkup Cybercrime	1
B. Pentingnya kajian hukum pidana dan perdata dalam cybercrime.....	3
C. Perkembangan teknologi dan tantangan hukum dalam tindak pidana cybercrime di Indonesia	6
BAB II DASAR HUKUM CYBERCRIME DI INDONESIA.....	10
A. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 11 Tahun 2008	10
B. Kitab Undang-Undang Hukum Pidana (KUHP) dan relevansinya..	13
C. Hukum perdata terkait perlindungan konsumen dan hak kekayaan intelektual (HaKI).....	17
D. Konvensi Internasional tentang Cybercrime (Budapest Convention 2001).....	20
BAB III JENIS-JENIS CYBERCRIME DALAM PERSPEKTIF HUKUM PIDANA	24
A. Tindak pidana terhadap kerahasiaan, integritas, dan ketersediaan data (illegal access, illegal interception).....	24
B. Penipuan dan pemalsuan data elektronik.....	26
C. Cyberterrorism dan Penyebaran Konten Illegal.....	31
D. Studi kasus dan putusan pengadilan terkait tindak pidana siber di Indonesia.....	39
BAB IV ASPEK HUKUM PERDATA DALAM CYBERCRIME	43
A. Perlindungan konsumen dalam transaksi elektronik (e-commerce)	43
B. Sengketa kontrak elektronik dan penyelesaian perdata	49
C. Perlindungan hak kekayaan intelektual di dunia maya.....	51
D. Tanggung Jawab Perdata Pelaku dan Penyedia Layanan Internet...	53
BAB V PENEGAKAN HUKUM DAN PROSES PERADILAN CYBERCRIME	56
A. Prosedur penyidikan dan penyelidikan tindak pidana siber.....	56
B. Pembuktian dan alat bukti elektronik dalam peradilan.....	59

C. Peran kepolisian siber, kejaksaan, dan pengadilan	61
D. Hambatan dan tantangan penegakan hukum lintas negara	62
BAB VI PERLINDUNGAN DAN PENCEGAHAN CYBERCRIME	64
A. Strategi pencegahan berbasis teknologi dan edukasi masyarakat....	64
B. Peran pemerintah, swasta, dan masyarakat sipil.....	65
C. Kerjasama internasional dalam pemberantasan cybercrime	66
BAB VII TINJAUAN YURIDIS DAN KEBIJAKAN	68
A. Evaluasi efektivitas UU ITE dan peraturan pendukung	68
B. Rekomendasi penguatan regulasi dan penegakan hukum.....	70
C. Implikasi Sosial dan Ekonomi dari Cybercrime	73
BAB VIII STUDI KASUS DAN CONTOH IMPLEMENTASI CYBERLAW (HUKUM SIBER).....	76
A. Studi Kasus Pelanggaran Data Pribadi	76
B. Studi Kasus Penipuan Transaksi Elektronik.....	79
C. Studi kasus pelanggaran hak cipta digital.....	81
BAB IX STRATEGI NASIONAL CYBERSECURITY (KEAMANAN SIBER)	84
A. Peran Badan Siber dan Sandi Negara (BSSN) sebagai koordinator nasional.....	84
B. Kerja sama internasional dan regional (misal: ASEAN Cybersecurity Cooperation).....	87
C. Reformasi hukum dan penguatan penegakan hukum terhadap kejahatan siber di Indonesia.....	89
DAFTAR REFERENSI.....	93
TENTANG PENULIS.....	108



BAB I

PENDAHULUAN

A. DEFINISI DAN RUANG LINGKUP *CYBERCRIME*

Cybercrime merupakan kejahatan yang dilakukan dengan menggunakan teknologi informasi dan komunikasi (Sulubara, 2024). Dalam konteks hukum, cybercrime tidak hanya berkaitan dengan tindak pidana, tetapi juga menimbulkan persoalan perdata, terutama terkait perlindungan hak dan kerugian yang dialami korban. UU ITE menjadi payung hukum utama dalam penanganan cybercrime di Indonesia, mengatur berbagai tindak pidana siber seperti akses ilegal, penyebaran konten negatif, dan penipuan elektronik (Onwuadiamu, 2025). Selain itu, hukum perdata mengatur sengketa kontrak elektronik dan perlindungan hak kekayaan intelektual yang seringkali menjadi objek sengketa di dunia maya (Sulubara, 2024).

Penegakan hukum cybercrime menghadapi tantangan dalam pembuktian elektronik dan yurisdiksi lintas negara (Okutan & Çebi, 2019). Peran aparat penegak hukum dan pengadilan sangat penting dalam memastikan keadilan bagi korban dan mencegah pelaku kejahatan siber. Pencegahan cybercrime memerlukan pendekatan multidisipliner, termasuk edukasi masyarakat, penguatan sistem keamanan teknologi, dan kerjasama internasional. Cybercrime atau kejahatan siber adalah tindakan melawan hukum yang dilakukan dengan menggunakan sistem elektronik atau teknologi informasi, termasuk internet dan komputer, yang bertujuan merugikan orang lain atau institusi baik secara materi maupun non-materi. Cybercrime dapat dilakukan untuk keuntungan pribadi, kelompok, atau sekadar memenuhi kepuasan pelaku (Alhadidi et al., 2024). Secara luas, tindak pidana siber mencakup semua tindak pidana yang menggunakan sarana atau bantuan sistem

elektronik. Ini berarti bahwa kejahatan konvensional seperti pembunuhan atau perdagangan orang juga dapat dikategorikan sebagai tindak pidana siber jika menggunakan teknologi elektronik sebagai sarana.

Menurut UU Informasi dan Transaksi Elektronik (UU ITE) No. 11 Tahun 2008 dan perubahannya UU No. 19 Tahun 2016, cybercrime mencakup berbagai perbuatan pidana yang terkait dengan penggunaan teknologi informasi, seperti hacking (meretas), intersepsi ilegal, pencurian data elektronik, penyebaran konten ilegal, dan pemalsuan identitas.. Ruang lingkup cybercrime meliputi dua kelompok utama (Okutan & Çebi, 2019):

1. Kejahatan yang menargetkan sistem dan teknologi. Ini termasuk perbuatan yang menyerang sistem komputer, jaringan, dan data elektronik, seperti:
 - a. Meretas (hacking).
 - b. Intersepsi ilegal (penyadapan).
 - c. Pengotoran situs (defacing).
 - d. Pencurian data elektronik.
 - e. Gangguan atau pengacauan sistem (interference).
 - f. Memfasilitasi tindak pidana lain melalui teknologi.
 - g. Pencurian identitas digital.
2. Kejahatan berbasis konten dan media elektronik. Meliputi penyebaran konten ilegal seperti:
 - a. Pornografi anak.
 - b. Penyebaran berita bohong (hoaks) dan ujaran kebencian.
 - c. Penghinaan dan pencemaran nama baik.
 - d. Pemerasan dan ancaman melalui media elektronik.
 - e. Perjudian dan aktivitas ilegal lainnya yang dilakukan secara online.

Selain itu, cybercrime juga mencakup tindak pidana yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP) yang menggunakan teknologi sebagai sarana, serta tindak pidana baru yang muncul seiring perkembangan teknologi digital. Cybercrime adalah segala bentuk kejahatan yang memanfaatkan teknologi informasi dan sistem elektronik untuk melakukan tindakan ilegal yang merugikan pihak lain. Ruang lingkungannya sangat luas, meliputi serangan terhadap sistem teknologi dan penyalahgunaan konten

digital, yang diatur dalam UU ITE serta hukum pidana lainnya di Indonesia (Bhushan, 2022).

Kajian hukum pidana dan perdata dalam konteks cybercrime sangat penting karena kejahatan siber merupakan fenomena yang kompleks dan berkembang pesat, yang melibatkan berbagai aspek hukum untuk penanganannya secara efektif. Pentingnya kajian hukum pidana dalam Cybercrime yaitu (Shah et al., 2019)

1. Hukum pidana berperan utama dalam memberikan dasar hukum untuk penindakan dan penegakan hukum terhadap pelaku kejahatan siber, seperti hacking, penipuan online, pencurian data, dan penyebaran konten ilegal.
2. Kajian hukum pidana membantu mengidentifikasi dan memperbarui regulasi yang adaptif dan komprehensif agar dapat menghadapi dinamika kejahatan siber yang semakin canggih dan intens.
3. Kebijakan hukum pidana yang tepat dapat meningkatkan efektivitas penanggulangan cybercrime, termasuk penguatan kapasitas aparat penegak hukum dan kerjasama internasional dalam menghadapi kejahatan lintas negara.
4. Kajian ini juga menyoroti perlunya revisi undang-undang seperti UU ITE untuk mengoptimalkan penegakan hukum terhadap kejahatan dunia maya di Indonesia.

B. PENTINGNYA KAJIAN HUKUM PIDANA DAN PERDATA DALAM *CYBERCRIME*

Cybercrime tidak hanya menimbulkan kerugian pidana, tetapi juga kerugian materiil dan immateriil yang berdampak pada hak-hak perdata seperti hak atas data pribadi, hak kekayaan intelektual, dan hak konsumen. Kajian hukum perdata diperlukan untuk memberikan perlindungan hukum terhadap kerugian tersebut dan memberikan mekanisme ganti rugi kepada korban (I. Seri Mughni Sulubara, 2024). Banyak kasus cybercrime, seperti penipuan online atau pencemaran nama baik di dunia maya, dapat diselesaikan melalui jalur perdata, misalnya gugatan ganti rugi atau tuntutan penghentian perbuatan melawan hukum (Onwuadiamu, 2025). Oleh karena itu, hukum perdata menjadi penting sebagai alternatif penyelesaian sengketa di luar proses pidana.

Hukum pidana berfokus pada penindakan pelaku kejahatan, sedangkan hukum perdata berperan dalam pemulihan hak korban dan kompensasi kerugian. Kajian hukum perdata melengkapi hukum pidana dalam memberikan keadilan menyeluruh bagi para pihak yang dirugikan akibat cybercrime. Cybercrime sering terjadi dalam konteks transaksi elektronik dan interaksi digital yang melibatkan kontrak, hak kekayaan intelektual, dan perlindungan data (Sarkar & Shukla, 2023). Hukum perdata mengatur aspek-aspek ini sehingga dapat mencegah dan mengatasi pelanggaran yang bersifat non-pidana namun merugikan secara hukum perdata.

Dalam perkembangan teknologi informasi yang cepat, sering terdapat celah hukum yang belum diatur secara tegas dalam hukum pidana. Kajian hukum perdata membantu menutup celah tersebut dengan memberikan dasar hukum untuk penanganan kerugian dan pelanggaran yang tidak selalu masuk ranah pidana. Hukum perdata berperan penting dalam perlindungan konsumen digital dan pengaturan perlindungan data pribadi, yang merupakan aspek krusial dalam mencegah dan menangani kejahatan siber seperti pencurian identitas dan penyalahgunaan data (A. A. Seri Mughni Sulubara, 2024). Kajian hukum perdata dalam cybercrime penting karena memberikan kerangka hukum yang komprehensif untuk melindungi hak-hak korban, menyelesaikan sengketa, serta melengkapi penegakan hukum pidana dalam menghadapi kompleksitas kejahatan di dunia maya. Alasan pentingnya kajian hukum perdata dalam cybercrime adalah (Alshaikhi, 2023):

1. Hukum perdata berperan dalam menangani aspek-aspek non-pidana dari cybercrime, seperti perlindungan hak cipta, hak kekayaan intelektual, perlindungan data pribadi, dan penyelesaian sengketa transaksi elektronik.
2. Kajian hukum perdata penting untuk memberikan perlindungan hukum kepada korban, misalnya dalam kasus pencurian data pribadi dan kerugian akibat transaksi elektronik yang merugikan.
3. Pengaturan hukum perdata juga menjadi dasar bagi penyelesaian sengketa di dunia maya yang melibatkan individu, perusahaan, dan institusi, sehingga menciptakan kepastian hukum dan keadilan di ranah digital.

Kajian hukum pidana dan perdata sangat krusial dalam penanggulangan cybercrime karena keduanya saling melengkapi: hukum pidana untuk penindakan dan pencegahan kejahatan siber, serta hukum perdata untuk perlindungan hak dan penyelesaian sengketa yang timbul dari aktivitas digital. Pembaharuan hukum, peningkatan kapasitas penegak hukum, serta edukasi dan kesadaran masyarakat menjadi kunci keberhasilan penanganan cybercrime secara menyeluruh. Perkembangan teknologi di Indonesia pada tahun 2025 menunjukkan kemajuan pesat di berbagai sektor seperti fintech, e-commerce, media sosial, Internet of Things (IoT), dan jaringan 5G yang menjadi tulang punggung transformasi digital nasional.

Namun, kemajuan ini juga menghadirkan tantangan hukum yang signifikan. Pengguna internet di Indonesia telah mencapai lebih dari 220 juta orang atau sekitar 80% dari total populasi, dengan penetrasi internet yang semakin merata hingga ke daerah pedesaan. E-commerce tumbuh pesat dengan nilai transaksi mencapai USD 100 miliar dan didukung oleh metode pembayaran digital yang semakin populer. E-commerce tumbuh pesat dengan nilai transaksi mencapai USD 100 miliar dan didukung oleh metode pembayaran digital yang semakin populer. AI semakin canggih dan mandiri, digunakan dalam berbagai sektor mulai dari layanan pelanggan hingga analisis risiko dan Kesehatan.

IoT berkembang pesat dengan jutaan perangkat terhubung yang mendukung smart city dan rumah pintar. Regulasi yang ada seringkali belum mampu mengimbangi kecepatan inovasi teknologi sehingga menjadi kurang relevan atau tidak efektif dalam mengatur teknologi baru. Perlindungan data pribadi dan keamanan siber menjadi isu utama, mengingat meningkatnya risiko kebocoran data, penyalahgunaan informasi, dan cybercrime. Kejahatan siber yang bersifat lintas negara memerlukan harmonisasi hukum dan kerja sama internasional yang kuat agar penegakan hukum dapat berjalan efektif. Kurangnya pemahaman teknis di kalangan pembuat kebijakan dan aparat penegak hukum menghambat pembuatan dan pelaksanaan regulasi yang tepat dan adaptif. Perlu reformasi hukum, termasuk pembaruan UU ITE dan penguatan perlindungan konsumen digital, untuk menyesuaikan dengan perkembangan teknologi seperti AI, blockchain, dan fintech (Li & Liu, 2021).

Perkembangan teknologi di Indonesia membuka peluang besar untuk kemajuan ekonomi dan sosial, namun juga menuntut sistem hukum yang

responsif dan adaptif. Tantangan hukum utama meliputi pembaruan regulasi, perlindungan data dan privasi, penanganan cybercrime, serta peningkatan kapasitas aparat penegak hukum. Kolaborasi antara pemerintah, sektor swasta, dan masyarakat menjadi kunci untuk mengatasi tantangan ini dan memaksimalkan manfaat teknologi bagi bangsa.

C. PERKEMBANGAN TEKNOLOGI DAN TANTANGAN HUKUM DALAM TINDAK PIDANA *CYBERCRIME* DI INDONESIA

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Nomor 11 Tahun 2008 adalah regulasi yang mengatur segala hal terkait informasi dan transaksi elektronik di Indonesia. UU ini berlaku bagi setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang ini, baik yang berada di dalam maupun di luar wilayah hukum Indonesia, selama perbuatannya memiliki akibat hukum di wilayah Indonesia dan/atau merugikan kepentingan Indonesia (Ferry et al., 2023). UU ITE dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati-hatian, iktikad baik, dan kebebasan memilih teknologi atau netral teknologi. Tujuan utama UU ini meliputi (Al-Nasrawi, 2021):

1. Mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat informasi dunia.
2. Mengembangkan perdagangan dan perekonomian nasional untuk meningkatkan kesejahteraan masyarakat.
3. Meningkatkan efektivitas dan efisiensi pelayanan publik.
4. Memberikan kesempatan seluas-luasnya kepada setiap orang untuk memajukan pemikiran dan kemampuan dalam penggunaan teknologi informasi secara optimal dan bertanggung jawab.
5. Memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara teknologi informasi.

UU ITE mengatur dua aspek besar yaitu informasi dan transaksi elektronik, serta perbuatan yang dilarang (cybercrime). Beberapa ketentuan penting antara lain (Cele & Kwenda, 2024):

1. Pengakuan informasi/dokumen elektronik sebagai alat bukti hukum yang sah (Pasal 5 dan 6).
2. Tanda tangan elektronik dan penyelenggaraan sertifikasi elektronik (Pasal 11-14).

3. Penyelenggaraan sistem elektronik (Pasal 15 dan 16).
4. Perbuatan yang dilarang (cybercrime), meliputi:
 - a. Konten ilegal seperti kesusilaan, perjudian, penghinaan atau pencemaran nama baik, pengancaman, dan pemerasan (Pasal 27-29).
 - b. Akses ilegal (Pasal 30).
 - c. Intersepsi ilegal (Pasal 31).
 - d. Gangguan terhadap data dan sistem elektronik (Pasal 32 dan 33).
 - e. Penyalahgunaan alat dan perangkat teknologi informasi (Pasal 34).

UU ITE telah mengalami revisi, salah satunya pada tahun 2016, yang mengubah beberapa ketentuan penting, khususnya terkait pasal penghinaan dan pencemaran nama baik. Revisi tersebut menegaskan bahwa pasal penghinaan adalah delik aduan, bukan delik umum, serta menurunkan ancaman pidana dan denda terkait pelanggaran tersebut. Selain itu, revisi juga menambahkan ketentuan mengenai "right to be forgotten" atau hak untuk dilupakan, yang memungkinkan penghapusan konten informasi elektronik yang tidak benar berdasarkan keputusan pengadilan (Artanto, 2023).

UU ITE merupakan landasan hukum utama dalam mengatur pemanfaatan teknologi informasi dan transaksi elektronik di Indonesia. UU ini memberikan kepastian hukum bagi pengguna dan penyelenggara teknologi, sekaligus mengatur larangan-larangan untuk mencegah dan menindak kejahatan siber. Revisi UU ITE terus dilakukan untuk menyesuaikan dengan perkembangan teknologi dan kebutuhan perlindungan hak masyarakat di era digital (Njatrijani, 2022). UU ITE merupakan landasan hukum utama dalam mengatur pemanfaatan teknologi informasi dan transaksi elektronik di Indonesia. UU ini memberikan kepastian hukum bagi pengguna dan penyelenggara teknologi, sekaligus mengatur larangan-larangan untuk mencegah dan menindak kejahatan siber. Revisi UU ITE terus dilakukan untuk menyesuaikan dengan perkembangan teknologi dan kebutuhan perlindungan hak masyarakat di era digital (Ketaren, 2017):

1. Pasal 27 ayat (3) UU ITE menyatakan bahwa setiap orang yang dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, atau membuat dapat diakses informasi elektronik dan/atau dokumen elektronik yang mengandung penghinaan dan/atau pencemaran nama baik dapat dipidana.

2. Pasal 28 ayat (2) UU ITE mengatur bahwa setiap orang yang dengan sengaja dan tanpa hak menyebarluaskan informasi elektronik yang mengandung penghinaan dan/atau pencemaran nama baik juga dapat dikenai sanksi pidana.
3. Sanksi pidana bagi pelanggaran Pasal 27 ayat (3) dapat berupa pidana penjara maksimal 6 tahun dan/atau denda maksimal Rp1 miliar, sedangkan pelanggaran Pasal 28 ayat (2) dapat dikenai pidana penjara maksimal 4 tahun dan/atau denda maksimal Rp750 juta.
4. UU ITE mengakui bahwa pencemaran nama baik dapat berupa tulisan, gambar, audio, atau bentuk lain yang dapat diakses secara elektronik, sehingga cakupannya luas dalam konteks media sosial dan internet.
5. Untuk dapat dikenai pasal ini, konten yang dianggap menghina atau mencemarkan nama baik harus jelas mengacu pada identitas orang pribadi tertentu, bukan pada kelompok umum atau anonim. Jika tidak ada kejelasan identitas korban, maka konten tersebut tidak dapat dikategorikan sebagai pencemaran nama baik menurut Pasal 27 ayat (3) UU ITE.
6. UU ITE menggabungkan prinsip-prinsip pencemaran nama baik dari KUHP ke ranah digital, sehingga unsur-unsur penghinaan dan pencemaran nama baik tetap merujuk pada definisi dalam KUHP, namun dengan penyesuaian pada media dan cara penyebarannya yang berbasis elektronik.
7. Proses hukum pencemaran nama baik online melibatkan pelaporan oleh korban kepada aparat penegak hukum, penyelidikan, penyidikan, dan penuntutan, dengan bukti elektronik seperti tangkapan layar, link, atau data elektronik lainnya sebagai alat bukti.

Singkatnya, UU ITE memberikan perlindungan hukum terhadap pencemaran nama baik di dunia digital dengan mengatur secara tegas larangan penyebaran informasi elektronik yang mengandung penghinaan atau pencemaran nama baik, disertai sanksi pidana yang cukup berat untuk mencegah penyalahgunaan media elektronik. Pasal 27 ayat (3) Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) memberikan perlindungan hukum yang kuat bagi korban pencemaran nama baik online dengan mengatur larangan bagi setiap orang yang dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, atau membuat dapat diakses

informasi elektronik yang mengandung penghinaan dan/atau pencemaran nama baik (Hilmy, Muhammad & Azmi, Rama, Halim, 2021). Berikut cara Pasal 27 ayat (3) UU ITE melindungi korban pencemaran nama baik online:

1. Landasan hukum untuk menuntut pelaku: Korban dapat mengajukan tuntutan pidana terhadap pelaku pencemaran nama baik yang merusak reputasi atau kehormatan mereka melalui media elektronik, seperti media sosial, website, atau platform digital lainnya.
2. Sanksi pidana yang tegas: Pelaku dapat dikenai hukuman pidana penjara hingga 4 tahun dan/atau denda maksimal Rp750 juta, sehingga memberikan efek jera dan perlindungan terhadap korban.
3. Pengakuan bukti elektronik: Pasal ini mengakui bukti elektronik seperti tangkapan layar, rekaman digital, dan data elektronik lainnya sebagai alat bukti yang sah dalam proses hukum, memudahkan korban untuk membuktikan pencemaran nama baik yang dialaminya.
4. Perlindungan terhadap pencemaran yang ditujukan kepada individu tertentu: Pasal ini mengacu pada konsep penghinaan dan pencemaran nama baik sebagaimana diatur dalam KUHP, sehingga harus ada unsur menyerang kehormatan atau nama baik seseorang secara spesifik dan dengan maksud untuk diketahui oleh umum.
5. Kemudahan identifikasi pelaku anonim: Dalam kasus pelaku menggunakan akun palsu atau anonim, Pasal 27 ayat (3) memungkinkan korban meminta bantuan penyedia layanan internet atau platform online untuk mengungkap identitas pelaku melalui proses hukum.
6. Pilihan hukum bagi korban: Korban dapat memilih untuk melaporkan kasus ke polisi untuk proses pidana atau mengajukan gugatan perdata guna mendapatkan ganti rugi atas kerugian yang dialami akibat pencemaran nama baik tersebut.

Pasal 27 ayat (3) UU ITE berfungsi sebagai payung hukum yang melindungi kehormatan dan nama baik seseorang di dunia digital, memberikan korban akses untuk menuntut keadilan dan mencegah penyebaran konten penghinaan atau pencemaran nama baik secara online.



BAB II

DASAR HUKUM CYBERCRIME DI INDONESIA

A. UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK (UU ITE) NO. 11 TAHUN 2008

Dasar hukum utama penanganan cybercrime di Indonesia adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahan yang diatur dalam Undang-Undang Nomor 19 Tahun 2016 (Koto, 2021). UU ITE mengatur berbagai tindak pidana yang berkaitan dengan kejahatan di dunia maya, seperti penyebaran informasi elektronik yang melanggar hukum, akses ilegal, intersepsi ilegal, dan gangguan terhadap sistem elektronik. Selain UU ITE, dasar hukum lainnya yang mendukung penanganan cybercrime di Indonesia meliputi (Purnama Santhi & Nuarta, 2023):

1. Kitab Undang-Undang Hukum Pidana (KUHP), yang mengatur tindak pidana umum yang juga dapat terjadi di ranah digital.
2. Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP), yang mengatur tata cara penyidikan dan penuntutan tindak pidana, termasuk tindak pidana siber.
3. Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana, yang relevan dalam pengaturan transaksi elektronik dan pencegahan kejahatan keuangan melalui teknologi informasi.

UU ITE mengatur tindak pidana materil dan formil yang memberikan landasan kuat bagi aparat penegak hukum untuk melakukan penyidikan dan penuntutan kasus cybercrime. Misalnya, Pasal 27 sampai Pasal 34 UU ITE mencakup berbagai jenis kejahatan siber, sementara Pasal 42 mengatur mekanisme penyidikan berdasarkan KUHAP dengan ketentuan khusus yang menjaga privasi dan kelancaran layanan public (Handoyo et al., 2024). Selain itu, dalam konteks perkembangan hukum terbaru, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP) juga mengatur tindak pidana siber secara lebih spesifik, seperti akses ilegal terhadap sistem elektronik, yang memberikan pelengkap dan penguatan terhadap UU ITE (Hikmatulloh & Nurmiati, 2020).

Singkatnya, dasar hukum cybercrime di Indonesia bersifat komprehensif dan melibatkan beberapa peraturan, dengan UU ITE sebagai landasan utama yang mengatur kejahatan di dunia digital serta prosedur penanganannya secara hukum pidana dan perdata (Gulo et al., 2021). Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 11 Tahun 2008 menjadi dasar hukum utama dalam penanganan cybercrime di Indonesia karena beberapa alasan berikut :

1. Pengaturan khusus tindak pidana siber. UU ITE secara eksplisit mengatur berbagai tindak pidana yang berkaitan dengan kejahatan di dunia maya, seperti penyebaran informasi elektronik yang melanggar hukum, akses ilegal (hacking), intersepsi ilegal, pencemaran nama baik online, penipuan daring, dan gangguan terhadap sistem elektronik. Pasal-pasal mulai dari Pasal 27 sampai Pasal 37 UU ITE memuat larangan dan sanksi pidana atas perbuatan-perbuatan tersebut.
2. Pengakuan informasi dan dokumen elektronik sebagai alat bukti. UU ITE mengakui informasi dan dokumen elektronik sebagai alat bukti hukum yang sah dalam proses peradilan, sehingga memudahkan penegakan hukum terhadap kejahatan siber yang menggunakan media digital.
3. Sanksi pidana yang tegas dan spesifik. UU ITE menetapkan ancaman pidana yang cukup berat, seperti pidana penjara dan denda, untuk berbagai bentuk kejahatan siber. Contohnya, Pasal 30 mengatur akses ilegal dengan ancaman hukuman hingga 7 tahun penjara, dan Pasal 28 mengatur intersepsi ilegal dengan ancaman maksimal 10 tahun penjara.

4. Landasan untuk penegakan hukum dan proses penyidikan. UU ITE memberikan dasar hukum bagi aparat penegak hukum untuk melakukan penyidikan dan penuntutan kasus cybercrime sesuai dengan ketentuan KUHAP, serta mengatur mekanisme perlindungan data dan privasi dalam proses tersebut.
5. Perubahan dan pembaruan UU ITE. UU ITE telah mengalami amandemen melalui UU No. 19 Tahun 2016 untuk menyesuaikan dengan perkembangan teknologi dan kebutuhan perlindungan hukum yang lebih baik. Hal ini menunjukkan UU ITE bersifat dinamis dan adaptif terhadap tantangan kejahatan siber yang terus berkembang.
6. Kerangka hukum yang komprehensif. Selain UU ITE, penanganan cybercrime juga didukung oleh peraturan pelaksana dan undang-undang lain seperti KUHP, KUHAP, dan UU Perlindungan Data Pribadi (UU PDP). Namun, UU ITE tetap menjadi payung hukum utama yang secara khusus mengatur aktivitas dan kejahatan di ranah elektronik.
7. Peran dalam meningkatkan kesadaran dan perlindungan masyarakat. UU ITE tidak hanya mengatur sanksi, tetapi juga memberikan kepastian hukum dalam transaksi elektronik dan perlindungan terhadap penyalahgunaan informasi, sehingga menjadi instrumen penting dalam melindungi masyarakat dari risiko kejahatan siber.

UU ITE No. 11 Tahun 2008 berfungsi sebagai landasan hukum utama yang mengatur dan menindak berbagai bentuk kejahatan siber di Indonesia dengan ketentuan yang spesifik, sanksi yang tegas, serta pengakuan bukti elektronik, sehingga menjadi instrumen vital dalam penegakan hukum cybercrime di era digital. Berikut adalah tindak pidana cyber yang diatur dalam Pasal 27 sampai Pasal 34 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 11 Tahun 2008 :

1. Pasal 27. Melarang setiap orang dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan:
 - Melanggar kesusilaan
 - Perjudian
 - Penghinaan dan/atau pencemaran nama baik

- Pemerasan dan/atau pengancaman
2. Pasal 28. Melarang penyebaran informasi elektronik dan/atau dokumen elektronik yang bermuatan:
 - Berita bohong yang merugikan konsumen dalam transaksi elektronik
 - Ujaran kebencian atau permusuhan berdasarkan SARA (Suku, Agama, Ras, dan Antar Golongan)
 3. Pasal 29. Melarang pengiriman ancaman kekerasan atau menakut-nakuti secara pribadi melalui sistem elektronik.
 4. Pasal 30. Melarang akses ilegal ke sistem elektronik milik orang lain tanpa hak atau melawan hukum (hacking).
 5. Pasal 31. Melarang intersepsi ilegal (penyadapan/transmisi tanpa hak) atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu.
 6. Pasal 32. Melarang perbuatan manipulasi, penciptaan, perubahan, penghilangan, atau perusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar data tersebut dianggap seolah-olah data yang otentik (defacing, pencurian data elektronik).
 7. Pasal 33. Melarang perbuatan yang menyebabkan terganggunya sistem elektronik dan/atau membuat sistem elektronik tidak bekerja sebagaimana mestinya (interference/disruption).
 8. Pasal 34. Melarang produksi, penjualan, pengadaan, penggunaan, impor, distribusi, penyediaan, atau kepemilikan perangkat keras atau perangkat lunak komputer, sandi komputer, kode akses, atau hal sejenis yang secara khusus dikembangkan untuk memfasilitasi tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai Pasal 33. Tindak pidana ini mencakup berbagai bentuk kejahatan digital, mulai dari penghinaan, penyebaran hoaks, hacking, pencurian data, hingga sabotase sistem elektronik dan penyediaan alat bantu untuk melakukan kejahatan siber

B. KITAB UNDANG-UNDANG HUKUM PIDANA (KUHP) DAN RELEVANSINYA

Kitab Undang-Undang Hukum Pidana (KUHP) adalah peraturan perundang-undangan yang mengatur mengenai perbuatan pidana secara materiil di Indonesia. KUHP yang berlaku saat ini merupakan warisan hukum

kolonial Belanda dan akan digantikan oleh Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana yang mulai berlaku pada 2 Januari 2026 (Sadino & Dewi, 2021). Terkait dengan cybercrime, KUHP secara umum mengatur tindak pidana konvensional, namun dalam konteks kejahatan siber, KUHP dapat diterapkan dalam arti luas apabila tindak pidana tersebut menggunakan sarana atau bantuan sistem elektronik. Misalnya, tindak pidana seperti pembunuhan atau perdagangan orang yang dilakukan dengan memanfaatkan sistem elektronik dapat dikategorikan sebagai tindak pidana siber menurut KUHP dalam arti luas (Anes et al., 2021).

Namun, pengaturan khusus mengenai cybercrime di Indonesia lebih rinci diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya, seperti UU No. 19 Tahun 2016. UU ITE mengatur berbagai tindak pidana yang berkaitan langsung dengan penggunaan teknologi informasi dan transaksi elektronik, seperti hacking, penyebaran malware, dan kejahatan digital lainnya (Swardhana, 2020). Singkatnya, dasar hukum cybercrime di Indonesia terdiri dari:

1. KUHP sebagai dasar hukum pidana umum yang juga dapat berlaku untuk tindak pidana yang menggunakan sarana elektronik dalam arti luas.
2. UU ITE sebagai regulasi khusus yang mengatur tindak pidana siber secara spesifik.
3. Beberapa undang-undang lain yang mendukung penanganan cybercrime, seperti UU Telekomunikasi, UU Pornografi, UU Perlindungan Konsumen, dan UU Tindak Pidana Pencucian Uang.

Dengan diberlakukannya KUHP baru (UU No. 1 Tahun 2023), diharapkan pengaturan pidana, termasuk yang terkait dengan teknologi dan kejahatan siber, dapat lebih sesuai dengan perkembangan zaman dan menjunjung hak asasi manusia. KUHP mengatur tindak pidana cyber di Indonesia melalui pasal-pasal khusus dalam KUHP baru (Undang-Undang Nomor 1 Tahun 2023) yang secara eksplisit mengatur kejahatan siber, memberikan landasan hukum yang lebih spesifik dan komprehensif dibandingkan sebelumnya. Beberapa contoh pengaturan dalam KUHP baru terkait tindak pidana cyber adalah (Al Asghor et al., 2024):

DAFTAR REFERENSI

Jurnal

- Abel, S., Mukarati, J., Manenge, R., & Le Roux, P. (2024). Evaluating bank technical efficiency in SADC region. *Heliyon*, 10(6), e27835. <https://doi.org/10.1016/j.heliyon.2024.e27835>
- Agustin, L. (2022). Evaluation of Factors influencing the Shopee PayLater adoption in Indonesia. *Management Science and Business Decisions*, 2(2), 5–18. <https://doi.org/10.52812/msbd.49>
- Aji, H. B. (2022). Pengaturan Jual Beli Secara Online Berdasarkan Undang-Undang Perlindungan Konsumen Dan Undang-Undang Informasi Dan Transaksi Elektronik. *Jurnal Hukum Progresif*, 10(1), 12–24. <https://doi.org/10.14710/jhp.10.1.12-24>
- Akub, M. S. (2020). Pengaturan Tindak Pidana Mayantara (Cyber Crime) Dalam Sistem Hukum Indonesia. *Al-Ishlah : Jurnal Ilmiah Hukum*, 21(2), 85–93. <https://doi.org/10.33096/aijih.v21i2.19>
- Al-Nasrawi, S. (2021). Combating Cyber Violence Against Women and Girls: An Overview of the Legislative and Policy Reforms in the Arab Region. *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, 493–512. <https://doi.org/10.1108/978-1-83982-848-520211037>
- Al Asghor, A., Arifin, M., & Minin, A. R. (2024). *Pertanggungjawaban Pidana Penipuan Trading Dengan Menyebarkan Berita Bohong Dalam Transaksi Elektronik*. 5(2), 304–311. <http://jurnal.bundamedia grup.co.id/index.php/iuris>
- Aldhaheeri, A., Alwahedi, F., Ferrag, M. A., & Battah, A. (2024). Deep learning for cyber threat detection in IoT networks: A review. *Internet of Things and Cyber-Physical Systems*, 4(September 2023), 110–128. <https://doi.org/10.1016/j.iotcps.2023.09.003>
- Alexandra, S., & Rosdiana. (2025). Reformasi Hukum Pidana dalam Menghadapi Kejahatan Transnasional: Studi Perbandingan Indonesia dan Uni Eropa. *Perkara : Jurnal Ilmu Hukum Dan Politik*, 3(1), 807–823. <https://doi.org/10.51903/perkara.v3i1.2344>

- Alhadidi, I., Nweiran, A., & Hilal, G. (2024). The influence of Cybercrime and legal awareness on the behavior of university of Jordan students. *Heliyon*, 10(12), e32371. <https://doi.org/10.1016/j.heliyon.2024.e32371>
- Alshaikhi, K. I. S. (2023). Meningkatkan Kapasitas Nasional Cybersecurity Authority (NCA) Kerajaan Arab Saudi untuk Memperkuat Keamanan Digital Nasional. *Lembaga Ketahanan Nasional Republik Indonesia*.
- Anes, G. A., Gosal, V. Y., & Rumimpunu, D. (2021). Tindak Pidana Tersangka Akses Ilegal Akun Instagram Yang Disita Penyidik Sebagai Alat Bukti Berdasarkan Kitab Undang-Undang Hukum Pidana. *Lex Privatum*, IX(13), 231–241.
- Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, 6(1), 132–142. <https://doi.org/10.38043/jah.v6i1.4484>
- Anita Sinaga, N. (2020). Pelanggaran Hak Merek Yang Dilakukan Pelaku Usaha Dalam Perdagangan Melalui Transaksi Elektronik (E-Commerce). *Jurnal Ilmiah Hukum Dirgantara*, 10(2), 76–95. <https://doi.org/10.35968/jh.v10i2.463>
- Arisandy, Y. O. (2021). Penegakan Hukum terhadap Cyber Crime Hacker. *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, 1(3), 162–169. <https://doi.org/10.18196/ijclc.v1i3.11264>
- Artanto. (2023). Transformasi Media Massa Untuk Membangun Opini Positif Guna Meningkatkan Ketahanan Nasional. *Lembaga Ketahanan Nasional Republik Indonesia*.
- Asimah, D. (2021). To Overcome the Constraints of Proof in the Application of Electronic Evidence. *Jurnal Hukum Peratun*, 3(2), 97–110. <https://doi.org/10.25216/peratun.322020.97-110>
- Ayman, D. N., & Nurhadiyanto, L. (2024). Analisis Kejahatan Siber Sniffing Pada Media Sosial Whatsapp (Studi Kasus Kurir Paket Bodong). *IKRA-ITH HUMANIORA: Jurnal ...*, 8(2), 373–384. <http://journals.upi-yai.ac.id/index.php/ikraith-humaniora/article/view/3693%0Ahttp://journals.upi-yai.ac.id/index.php/ikraith-humaniora/article/download/3693/2783>

- Azrica, H., & Sulubara, S. M. (2023). Legalitas Transaksi E Commerce Dalam Platfortm Shopee Ditinjau Dalam Kitab Undang-Undang Hukum Perdata (Burgerlijk Wetboek), Undang-Undang Nomor: 8 Tahun 1999 Tentang Perlindungan Konsumen Dan Perspektif Fiqih Muamalah. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, 1(3), 1–23. <https://doi.org/https://doi.org/10.51903/hakim.v1i3.1305>
- Bakry, M., Syatar, A., Abubakar, A., Risal, C., Ahmad, A., & Amiruddin, M. M. (2021). Strengthening the Cyber Terrorism Law Enforcement in Indonesia: Assimilation from Islamic Jurisdiction. *International Journal of Criminology and Sociology*, 10, 1267–1276. <https://doi.org/10.6000/1929-4409.2021.10.146>
- Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers and Security*, 111, 102490. <https://doi.org/10.1016/j.cose.2021.102490>
- Bhushan, T. (2022). Cyberlaw and cyberspace vis-a-vis impact of internet during COVID-19 pandemic. *World Journal of Engineering*, 19(1), 114–117. <https://doi.org/10.1108/WJE-01-2021-0029>
- Cabaj, K., Kotulski, Z., Księżopolski, B., & Mazurczyk, W. (2018). Cybersecurity: trends, issues, and challenges. *Eurasip Journal on Information Security*, 2018(1), 10–12. <https://doi.org/10.1186/s13635-018-0080-0>
- Cele, N. N., & Kwenda, S. (2024). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*, 32(1), 31–48. <https://doi.org/10.1108/JFC-10-2023-0263>
- Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. *Jurnal Politika Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, 10(2), 113–128. <https://doi.org/10.22212/jp.v10i2.1447>
- CSA Teddy Lesmana, Elis, E., & Hamimah, S. (2022). Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia.

Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia, 3(2), 1–6.
<https://doi.org/10.52005/rechten.v3i2.78>

- Duarif, D., & Saleh, M. (2024). Pencegahan dan Penindakan Tindak Pidana Siber oleh Kepolisian Resort Teluk Bintuni. *UNES Law Review*, 6(4), 12110–12119.
- Fadli, M., Widijowati, D., & Andayani, D. (2024). Pencurian Data Pribadi di Dunia Maya (Phising Cybercrime) yang ditinjau dalam Perspektif Kriminologi. *Co-Value Jurnal Ekonomi Koperasi Dan Kewirausahaan*, 14(12). <https://doi.org/10.59188/covalue.v14i11.4335>
- Fauzi, R., Ramli, T. S., & Permata, R. R. (2022). Masa Depan Hak Cipta: Tinjauan Keabsahan Hasil Karya Kecerdasan Artifisial Di Indonesia. *Citizen : Jurnal Ilmiah Multidisiplin Indonesia*, 2(1), 118–128. <https://doi.org/10.53866/jimi.v2i1.51>
- Febriyanti, A. (2024). Perlindungan Hukum Terhadap Kepemilikan Non-Fungible Token Sebagai Hak Kekayaan Intelektual. *JLEB: Journal of Law, Education and Business*, 2(1), 403–411. <https://doi.org/10.57235/jleb.v2i1.1743>
- Fernandez, E. B., & Romero, V. M. (2022). A security reference architecture for cargo ports. *Internet of Things and Cyber-Physical Systems*, 2(July), 120–137. <https://doi.org/10.1016/j.iotcps.2022.07.001>
- Ferrag, M. A., Alwahedi, F., Battah, A., Cherif, B., Mechri, A., Tihanyi, N., Bisztray, T., & Debbah, M. (2025). Generative AI in cybersecurity: A comprehensive review of LLM applications and vulnerabilities. *Internet of Things and Cyber-Physical Systems*, 5(October 2024), 1–46. <https://doi.org/10.1016/j.iotcps.2025.01.001>
- Ferry, I., Febriansyah, A., Ferry, *, Febriansyah, I., Indiantoro, A., & Ikhwan, A. (2023). Legal Standing Jurnal Ilmu Hukum Model Kejahatan Dunia Maya (Cybercrime) Sebagai Upaya Pembentukan Hukum Nasional. *Issn (E)*, 7(2), 2580–3883.
- Fista, Y. L., Aris Machmud, & Suartini, S. (2023). Perlindungan Hukum Konsumen Dalam Transaksi E-commerce Ditinjau dari Perspektif Undang-Undang Perlindungan Konsumen. *Binamulia Hukum*, 12(1), 177–189. <https://doi.org/10.37893/jbh.v12i1.599>

- Gajah, E. E., Fernando, F. F., Vadia, N., Ie, V. E., & Gumintang, G. G. (2023). Perlindungan Hukum bagi Pemegang Uang Elektronik (E-Money) Bermasalah Ditinjau Dari Undang-Undang Tentang Perlindungan Konsumen dan Undang-Undang Tentang Informasi dan Transaksi Elektronik. *Jurnal Kewarganegaraan*, 7(2), 2109–2120.
- Ghouse, G., Ejaz, N., Bhatti, M. I., & Aslam, A. (2022). Performance of islamic vs conventional banks in OIC countries: Resilience and recovery during Covid-19. *Borsa Istanbul Review*, 22, S60–S78. <https://doi.org/10.1016/j.bir.2022.11.020>
- Ginanjjar, Y. (2022). Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara. *Jurnal Dinamika Global*, 7(02), 291–312. <https://doi.org/10.36859/jdg.v7i02.1187>
- Gruber, J., Voigt, L. L., Benenson, Z., & Freiling, F. C. (2022). Foundations of cybercriminalistics: From general process models to case-specific concretizations in cybercrime investigations. *Forensic Science International: Digital Investigation*, 43, 301438. <https://doi.org/10.1016/j.fsidi.2022.301438>
- Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal of Criminal Law*, 1(2), 68–81. <https://doi.org/10.22437/pampas.v1i2.9574>
- Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, 23(2), 400–426. <https://doi.org/10.15642/alqanun.2020.23.2.400-426>
- Handoyo, B., MZ, H., Rahma, I., & Asy'ari. (2024). Tinjauan Yuridis Penegakkan Hukum Kejahatan Cyber Crime Studi Implementasi Undang-Undang Nomor 11 Tahun 2008. *MAQASIDI: Jurnal Syariah Dan Hukum*, 4(1), 40–55. <https://doi.org/10.47498/maqasidi.v4i1.2966>
- Hapsari, R. D., & Pambayun, K. G. (2023). ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Konstituen*, 5(1), 1–17. <https://doi.org/10.33701/jk.v5i1.3208>

- Haryanto, A., & Sutra, S. M. (2023). Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020. *Global Political Studies Journal*, 7(1), 56–69. <https://doi.org/10.34010/gpsjournal.v7i1.8141>
- Hasan, Z., Alfath, M. R., Mahardika, A., Rizaldi, R., & Rizqullah, W. (2024). Peranan Cyber Law Dalam Penanganan Tindak Pidana Di Indonesia. *Jurnal Komunikasi*, 2(5), 337–345.
- Helmawansyah, M. (2019). Penggunaan Barang Bukti Elektronik yang Dijadikan Alat Bukti dalam Perkara Pidana. *Journal of Law (Jurnal Ilmu Hukum)*, 6(1), 527–541.
- Herlambang, P. H., Utama, Y. J., & Putrijanti, A. (2024). Harmonisasi Hukum UU Peratun dan UU ITE dalam Ketentuan Alat Bukti Elektronik sebagai Alat Bukti Tambahan dalam Sistem Peradilan Tata Usaha Negara. *Jurnal Pembangunan Hukum Indonesia*, 6(1), 61–81.
- Hikmatulloh, R., & Nurmiati, E. (2020). Analisis Strategi Pencegahan Cybercrime Berdasarkan UU ITE Di Indonesia (Studi Kasus: Penipuan Pelanggan Gojek). *Kosmik Hukum*, 20(2), 121. <https://doi.org/10.30595/kosmikhukum.v20i2.6449>
- Hilmy, Muhammad, I., & Azmi, Rama, Halim, N. (2021). Konstruksi Pertahanan dan Keamanan Negara Terhadap Perlindungan Data dalam Cyberspace Untuk Menghadapi Pola Kebiasaan Baru. *Jurnal Lembaga Ketahanan Nasional Republik Indonesia*, 9(1), 114–124.
- Hisbulloh, M. H. (2021). Urgensi Rancangan Undang-Undang (Ruu) Perlindungan Data Pribadi. *Jurnal Hukum Unissula*, 37(2), 119–133. <https://doi.org/10.26532/jh.v37i2.16272>
- Hossain, M. A., & Islam, M. S. (2024). Enhanced detection of obfuscated malware in memory dumps: a machine learning approach for advanced cybersecurity. *Cybersecurity*, 7(1). <https://doi.org/10.1186/s42400-024-00205-z>
- Hu, C., Wu, T., Liu, C., & Chang, C. (2024). Joint contrastive learning and belief rule base for named entity recognition in cybersecurity. *Cybersecurity*, 7(1). <https://doi.org/10.1186/s42400-024-00206-y>
- Iftikhar, S. (2024). Cyberterrorism as a global threat: a review on repercussions and countermeasures. *PeerJ Computer Science*, 10. <https://doi.org/10.7717/peerj-cs.1772>

- Jacobsen, J. T. (2022). Cyberterrorism: Four Reasons for Its Absence—So Far. *Perspectives on Terrorism*, 16(5), 62–72.
- Judijanto, L., & Nugroho, B. (2025). Regulasi Keamanan Siber dan Penegakan Hukum terhadap Cybercrime di Indonesia. *Sanskara Hukum Dan HAM*, 3(03), 118–124. <https://doi.org/10.58812/shh.v3i03.544>
- Ketaren, E. (2017). Cybercrime, Cyber Space, Dan Cyber Law. *Jurnal TIMES*, 5(2), 35–42. <https://doi.org/10.51351/jtm.5.2.2016556>
- Koto, I. (2021). Cyber Crime According to the ITE Law. *International Journal Reglement & Society (IJRS)*, August, 103–110. <https://doi.org/10.55357/ijrs.v2i2.124>
- Latifah Soroinda, D., & Annisa Rininta Soroinda Nasution, A. (2022). Kekuatan Pembuktian Alat Bukti Elektronik Dalam Hukum Acara Perdata. *Jurnal Hukum & Pembangunan*, 52(2), 384–405. <https://scholarhub.ui.ac.id/jhpAvailableat:https://scholarhub.ui.ac.id/jhp/vol52/iss2/4>
- Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7, 8176–8186. <https://doi.org/10.1016/j.egyr.2021.08.126>
- Ma'arif, S., Ibda, H., Ahmadi, F., Qosim, N., & Muanayah, N. A. (2023). Islamic moderation in education and the phenomenon of cyberterrorism: a systematic literature review. *Indonesian Journal of Electrical Engineering and Computer Science*, 31(3), 1523–1533. <https://doi.org/10.11591/ijeecs.v31.i3.pp1523-1533>
- Malau, P. (2023). Tinjauan Kitab Undang-Undang Hukum Pidana (KUHP) Baru 2023. *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam*, 5(1), 837–844. <https://doi.org/10.37680/almanhaj.v5i1.2815>
- Manurung, E. A. P., & Thalib, E. F. (2022). Tinjauan Yuridis Perlindungan Data Pribadi Berdasarkan Uu Nomor 27 Tahun 2022. *Jurnal Hukum Saraswati (JHS)*, 4(2), 139–148.
- Markus Djarawula, Novita Alfiani, & Hanita Mayasari. (2023). Tinjauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime) Di Indonesia Ditinjau Dari Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Jurnal Cakrawala Ilmiah*, 2(10), 3799–3806. <https://doi.org/10.53625/jcijurnalcakrawalailmiah.v2i10.5842>

- Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers and Security*, 120. <https://doi.org/10.1016/j.cose.2022.102820>
- Muhammad Fahad. (2023). Perlindungan Konsumen Dalam Perjanjian Jual Beli Online. *Journal Sains Student Research*, 1(2), 1043–1050. <https://doi.org/10.61722/jssr.v1i2.390>
- Mulyanti, N. R., & Widyowati, D. S. (2023). Tinjauan Hukum Ekonomi Syariah Terhadap ShopeePay Later. *Jurnal Ilmu Syariah Dan Hukum (JISYAKU)*, 2(2), 137–147. <https://doi.org/10.23971/jisyaku.v2i2.6870>
- Mursidi, H. (2019). Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Cyber Crime Phising (Studi Kasus Putusan Pengadilan Negeri Medan Nomor: 3006/Pid. Sus *Skripsi, Fakultas Hukum Universitas Sriwijaya* https://repository.unsri.ac.id/24793/50/RAMA_74201_0201138141934_8_0018096509_0003117704_01_front_ref.pdf
- Njatrijani, R. (2022). Law , Development & Justice Review Law , Development & Justice Review. *Law, Development & Justice Review*, 3(2), 1–9.
- Okutan, A., & Çebi, Y. (2019). A Framework for Cyber Crime Investigation. *Procedia Computer Science*, 158, 287–294. <https://doi.org/10.1016/j.procs.2019.09.054>
- Onwuadiamu, G. (2025a). Cybercrime in criminology; A systematic review of criminological theories, methods, and concepts. *Journal of Economic Criminology*, 8(February), 100136. <https://doi.org/10.1016/j.jeconc.2025.100136>
- Onwuadiamu, G. (2025b). Cybercrime in criminology; A systematic review of criminological theories, methods, and concepts. *Journal of Economic Criminology*, 8(December 2024), 100136. <https://doi.org/10.1016/j.jeconc.2025.100136>
- Paminto, S. R. (2022). Cyber Terrorism Countermeasures in Indonesia. *Jurnal Wawasan Yuridika*, 6(2), 186–196. <https://doi.org/10.25072/jwy.v6i2.464>

- Pansariadi, R. S. B., & Soekorini, N. (2023). Tindak Pidana Cyber Crime dan Penegakan Hukumnya. *Binamulia Hukum*, 12(2), 287–298. <https://doi.org/10.37893/jbh.v12i2.605>
- Popal, D. F. T. (2023). Upaya Penanggulangan Tindak Pidana Mayantara (Cyber Crime). *Lex Administratum*, 5. <https://ejournal.unsrat.ac.id/index.php/administratum/article/view/51005%0Ahttps://ejournal.unsrat.ac.id/index.php/administratum/article/download/51005/43956>
- Purnama Santhi, N. N. P., & Nuarta, I. N. (2023). Penguatan Penegakan Hukum Polri dalam Rangka Optimalisasi Penanggulangan Cybercrime di Indonesia. *SCIENTIA: Journal of Multi Disciplinary Science*, 2(1), 15–27. <https://doi.org/10.62394/scientia.v2i1.40>
- Purwadi, A., Serfiyani, C. Y., & Serfiyani, C. R. (2022). Legal Landscape on National Cybersecurity Capacity in Combating Cyberterrorism Using Deep Fake Technology in Indonesia. *International Journal of Cyber Criminology*, 16(1), 123–140. <https://doi.org/10.5281/zenodo.4766560>
- Qarani, M. T., & Suminar, S. R. (2022). Penyelesaian Wanprestasi Pinjam-Meminjam Shopeepaylater Ditinjau dari Buku III KUHPerdato Jo Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan *Bandung Conference Series* ..., 585–592. <https://proceedings.unisba.ac.id/index.php/BCSLs/article/view/1004>
- Rachmadie, D. T., & Supanto, '. (2020). Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Udang Republik Indonesia Nomor 19 Tahun 2016. *Recidive : Jurnal Hukum Pidana Dan Penanggulangan Kejahatan*, 9(2), 128. <https://doi.org/10.20961/recidive.v9i2.47400>
- Rahaditya, R., Goldwen, F., Fernandha, R. D., Octavia S, C., Aryadi, A. M., & Rahmasari, L. (2023). Tinjauan Yuridis Hak Atas Merek Sebagai Hak Kekayaan Intelektual. *Jurnal Sosial Humaniora Sigli*, 6(2), 747–760. <https://doi.org/10.47647/jsh.v6i2.2040>
- Rahmawati, I. (2017). the Analysis Ofcyber Crime Threat Risk Management To Increase Cyber Defense. *Jurnal Pertahanan & Bela Negara*, 7(2), 51–66. <https://doi.org/10.33172/jpbh.v7i2.193>

- Ramadhan, G. (2023). Perlindungan Hukum Bagi Korban Ransomware Wannacry Tindak Pidana Ransomware. *Jurnal Kajian Kontemporer Hukum Dan Masyarakat*, 01(02), 1–15. <https://doi.org/10.11111/dassollen.xxxxxxx>
- Rao, A. R., & Elias-Medina, A. (2024). Designing an internet of things laboratory to improve student understanding of secure IoT systems. *Internet of Things and Cyber-Physical Systems*, 4(September 2023), 154–166. <https://doi.org/10.1016/j.iotcps.2023.10.002>
- Rusmawati, D. E. (2015). Perlindungan Hukum Bagi Konsumen Dalam Transaksi E-Commerce. *FIAT JUSTISIA: Jurnal Ilmu Hukum*, 7(2). <https://doi.org/10.25041/fiatjustisia.v7no2.378>
- Sadino, S., & Dewi, L. K. (2021). Internet Crime Dalam Perdagangan Elektronik. *Jurnal Magister Ilmu Hukum*, 1(2), 9. <https://doi.org/10.36722/jmih.v1i2.732>
- Safa Meidiosa, N., & Lolita Permanasari. (2023). Perlindungan Hukum Pengguna Paylater Apabila Terjadi Wanprestasi (Studi Kasus Di Shopee Paylater). *Jurnal Hukum Dan Keadilan*, 12(8), 79–96. <https://doi.org/10.56943/judiciary.v12i1.147>
- Safsafubun, P. H., & Bustani, S. (2023). Analisis Perlindungan Konsumen Terhadap Transaksi Elektronik Pada Lembaga Perbankan Berdasarkan Peraturan No. 6/POJK. 07/2022. *Jurnal Ilmiah Mahasiswa Pendidikan* ..., 8(4), 4683–4696. <https://jim.usk.ac.id/sejarah/article/view/26824%0Ahttps://jim.usk.ac.id/sejarah/article/viewFile/26824/12583>
- Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. In *Journal of Big Data* (Vol. 11, Issue 1). Springer International Publishing. <https://doi.org/10.1186/s40537-024-00957-y>
- Salsabila, D., & Ispriyarso, B. (2023). Efektivitas Keabsahan Kontrak Elektronik Berdasarkan Hukum Positif di Indonesia. *AL-MANHAIJ: Jurnal Hukum Dan Pranata Sosial Islam*, 5(2), 1343–1354. <https://doi.org/10.37680/almanhaj.v5i2.3085>

- Sarihim, & Leo Alexander Tambunan. (2022). Pengaruh Paylater Terhadap Keputusan Pembelian Kembali Produk Di E-Commerce Shopee. *Jurnal Ilmiah Manajemen, Ekonomi Dan Bisnis*, 1(2), 17–20. <https://doi.org/10.51903/jimeb.v1i2.343>
- Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology*, 2(September), 100034. <https://doi.org/10.1016/j.jeconc.2023.100034>
- Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data*, 7(1). <https://doi.org/10.1186/s40537-020-00318-5>
- Seri Mughni Sulubara, Hidayati Purnama Lubis, Nanci Yosepin Simbolon, F. R. (2024). *Teori Hukum Perdata (Studi Kasus: Transaksi E-Commerce Shopee Paylater*. CV. Tahta Media Group.
- Seri Mughni Sulubara. (2024). Perlindungan Data Pribadi dalam Kasus Ransomware : Apa Kata Hukum ? *Eksekusi: Jurnal Ilmu Hukum Dan Administrasi Negara*, 2(November), 426–434. <https://doi.org/https://doi.org/10.55606/eksekusi.v2i4.1823>
- Seri Mughni Sulubara, A. A. (2024). Legalitas Fintech Peer To Peer Lending Pinjaman Online dalam Aspek Hukum Konvensional. *MANDUB: Jurnal Politik, Sosial, Hukum Dan Humaniora*, 2(2), 177–187. <https://doi.org/https://doi.org/10.59059/mandub.v2i2.1184>
- Seri Mughni Sulubara, A. A. (2024). Legalitas Fintech Peer To Peer Lending Pinjaman Online dalam Aspek Hukum Konvensional. *Universitas Muhammadiyah Mahakarya Aceh, Jalan Gayo Simpang IV Bireun Nomor: 2 Aceh*, 2(2).
- Seri Mughni Sulubara, I. (2024). Regulasi dan Lisensi Mengenai Perlindungan Hukum Investor di Platform Fintech Peer-To-Peer Lending dalam Hukum Konvensional. *Jurnal Hukum, Politik Dan Ilmu Sosial*, 3(4), 431–442. <https://doi.org/https://doi.org/10.55606/jhpis.v3i4.4499>
- Setiawan, D. A. (2020). Cyber Terrorism and its Prevention in Indonesia. *Jurnal Media Hukum*, 27(2), 267–283. <https://doi.org/10.18196/jmh.20200156>

- Setiawan, H. B., & Najicha, F. U. (2022). Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data. *Jurnal Kewarganegaraan*, 6(1), 976–982.
- Shah, M. H., Jones, P., & Choudrie, J. (2019). Cybercrimes prevention: promising organisational practices. *Information Technology and People*, 32(5), 1125–1129. <https://doi.org/10.1108/ITP-10-2019-564>
- Shandler, R., Kostyuk, N., & Oppenheimer, H. (2023). Public Opinion and Cyberterrorism. *Public Opinion Quarterly*, 87(1), 92–119. <https://doi.org/10.1093/poq/nfad006>
- Singgi, I. G. A. S. K., Suryawan, I. G. B., & Sugiarta, I. N. G. (2020). Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (Cyber Crime). *Jurnal Konstruksi Hukum*, 1(2), 334–339. <https://doi.org/10.22225/jkh.2.1.2553.334-339>
- Sitorus, F. M., Amirulloh, M., & Djukardi, E. H. (2022). Status Hak Kebendaan Atas Virtual Property Serta Keabsahan Real Money Trading yang Dilakukan Oleh Para Pemain Dalam Permainan Mobile Legends Ditinjau Dari Hukum Perdata Dan Cyber Law Indonesia. *Jurnal Sains Sosio Humaniora*, 6(1), 109–124. <https://doi.org/10.22437/jssh.v6i1.19399>
- Sukinta. (2020). Peran Kepolisian Dalam Melakukan Penyidikan Tindak Pidana Penyebaran Berita Bohong di Indonesia. *Online Administrative Law & Governance Journal*, 3(3), 2621–2781.
- Sulistianingsih, D., Ihwan, M., Setiawan, A., & Prabowo, M. S. (2023). Tata Kelola Perlindungan Data Pribadi Di Era Metaverse (Telaah Yuridis Undang-Undang Perlindungan Data Pribadi). *Masalah-Masalah Hukum*, 52(1), 97–106. <https://doi.org/10.14710/mmh.52.1.2023.97-106>
- Sulubara, S. M. (2023). Pendidikan Hukum Financial Technology Peer to Peer Lending (P2P). 1(3), 70–81.
- Sulubara, S. M. (2024). Menyajikan Berbagai Insiden Cybercrime yang Terjadi di Indonesia , Termasuk Pencurian Data dan Peretasan Situs Web Pemerintah. *Konsensus: Jurnal Ilmu Politik Dan Komunikasi*, 1(6), 199–206. <https://doi.org/https://doi.org/10.62383/konsensus.v1i6.692>

- Sulubara, S. M. (2024). Perlindungan Data Pribadi dalam Kasus Ransomware : Apa Kata Hukum ? *Eksekusi: Jurnal Ilmu Hukum Dan Administrasi Negara*, 2(4), 426–434. <https://doi.org/DOI:https://doi.org/10.55606/eksekusi.v2i4.1823>
- Sulubara, S. M., Basri, T. S., & . F. (2023). Legal Aspects of E-Commerce Agreements in Shopee Platform in The Civil Law Code (Burgerlijk Wetboek). *International Journal of Research and Review*, 10(6), 690–699. <https://doi.org/10.52403/ijrr.20230683>
- Sulubara, S. M., Fauzi, H., Muslim, B., Ferdiansyah, M. F., & Musmulyadi, M. (2025). Judi Online Sebagai Cybercrime Serta Tantangan Penegakan Hukum Pidana di Era Digital: Antara Regulasi , Pembuktian , dan Ancaman Cybercrime Universitas Muhammadiyah Mahakarya Aceh , Indonesia Sekolah Tinggi Ilmu Hukum Muhammadiyah Takengon , Indonesia di. *Jurnal Riset Rumpun Ilmu Sosial, Politik Dan Humaniora*, 4(2), 539–552. <https://doi.org/https://doi.org/10.55606/jurrish.v4i2.4990>
- Sulubara, S. M., Lubis, H. P., & Simbolon, N. Y. (2024). Legal Review of Electronic Commerce-Based Buying and Selling on the Shopee Platform Against Consumers Using Shopee PayLater. *Proceeding of IROFONIC 2024, Proceeding(02)*, 392–402.
- Sulubara, S. M., Lubis, H. P., & Simbolon, N. Y. (2024). Legality Of Shopee Paylater Payments For Shopee Platform E-Commerce Transactions In Conventional Law. *DELEGALATA Jurnal Ilmu Hukum*, 9(2), 247–256. <https://doi.org/10.30596/dll.v9i2.20414>
- Sutra Disemadi, H., & Kang, C. (2021). Tantangan Penegakan Hukum Hak Kekayaan Intelektual dalam Pengembangan Ekonomi Kreatif di Era Revolusi Industri 4.0. *Jurnal Komunikasi Hukum (JKH)*, 7(1), 54. <https://doi.org/10.23887/jkh.v7i1.31457>
- Sutrisno, S., & Astuti, I. (2024). Pengaruh Penerapan Standar Akuntansi Pemerintahan Dan Kualitas Laporan Keuangan Terhadap Akuntabilitas Kinerja Instansi Pemerintah Pada Badan Siber Dan Sandi Negara. *Aliansi : Jurnal Manajemen Dan Bisnis*, 18(2), 185–198. <https://doi.org/10.46975/aliansi.v18i2.532>
- Swardhana, G. M. (2020). Kebijakan Kriminal Dalam Menghadapi Perkembangan Kejahatan Cyber Adultery. *Kertha Wicaksana*, 14(2), 87–95. <https://doi.org/10.22225/kw.14.2.1844.87-95>

- Syarifuddin, Teresia Din, Tri Andriani, Antonius Rino Vanchapo, Hezron Sabar Rotua Tinambunan, D. K. S. (2024). Reformasi Hukum di Era Digital : *Indonesian Research Journal on Education*, 4, 3206–3215.
- Tampubolon, W. S. (2019). Perlindungan Konsumen Terhadap Pembelian Barang Melalui Media Jual Beli Online Ditinjau Dari Undang Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Uu Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Jurnal Ilmiah Advokasi*, 7(2), 98–108. <https://doi.org/10.36987/jiad.v7i2.1310>
- Ubaidillah. (2020). Analisis Hukum Islam terhadap Shopee Paylater Pada Sistem Jual Beli Online. *Jurnal Ekonomi Dan Hukum Islam*, 7(1), 53–65. <https://doi.org/10.35316/istidlal.v7i1.163>
- Umami, S. H., & Fithry, A. (2024). Mekanisme Penyidikan Dan Penuntutan Tindak Pidana Cybercrime: Tinjauan Hukum Indonesia. *Prosiding SNAPP : Sosial Humaniora, Pertanian, Kesehatan Dan Teknologi*, 2(1), 114–120. <https://doi.org/10.24929/snapp.v2i1.3129>
- Wei-Jung, C. (2020). Cyberstalking and law enforcement. *Procedia Computer Science*, 176, 1188–1194. <https://doi.org/10.1016/j.procs.2020.09.115>
- Widijowati, D. (2022). Legal Complexity in Dealing with Cyber Crime in Indonesia. *Research Horizon*, 2(6), 597–606.
- Wulandari, D., & Subagio, A. (2015). Consumer Decision Making in Conventional Banks and Islamic Bank based on Quality of Service Perception. *Procedia - Social and Behavioral Sciences*, 211(September), 471–475. <https://doi.org/10.1016/j.sbspro.2015.11.062>
- Yudaruddin, R., soedarmono, wahyoe, Nugroho, B. A., Fitriani, Z., Mardiany, M., Purnomo, A. H., & Santi, E. N. (2023). Financial technology and bank stability in an emerging market economy. *Heliyon*, 9(5), e16183. <https://doi.org/10.1016/j.heliyon.2023.e16183>
- Zhang, J., Bu, H., Wen, H., Chen, Y., Li, L., & Zhu, H. (2024). When LLMs Meet Cybersecurity: A Systematic Literature Review. *Cybersecurity*. <https://doi.org/10.1186/s42400-025-00361-w>

Peraturan PerUndang-Undangan

Kitab Undang-Undang Hukum Pidana (KUHP)

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan
Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi
dan Transaksi Elektronik

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Undang-undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen

Rancangan Undang-Undang Keamanan dan Ketahanan Siber

TENTANG PENULIS

Seri Mughni Sulubara, S.H., M.H



Seri Mughni Sulubara, S.H., M.H, lahir di Medan, 18 Desember 1986. Beliau menyelesaikan S-1 dan S-2 Magister Hukum konsentrasi hukum Perdata/Bisnis di Universitas Sumatera Utara, Medan. Saat ini beliau bekerja sebagai dosen tetap Fakultas Ilmu Sosial dan Humaniora Program Studi Ilmu Hukum Universitas Muhammadiyah Mahakarya Aceh, Bireun. Beliau aktif dalam mengerjakan kegiatan catur dharma dalam bidang muhammadiyah, pendidikan, penelitian dan pengabdian masyarakat. Saat ini beliau memiliki berbagai publikasi ilmiah jurnal penelitian dan pengabdian masyarakat terakreditasi nasional dan internasional. Beliau pun aktif menulis buku referensi, buku monograf, buku ajar, prosiding nasional dan internasional terpublikasi.

Viridya Tasril, S.Kom., M.Kom



Viridya Tasril, lahir di Padang, tanggal 13 Agustus 1991. Pada tahun 2013 menyelesaikan kuliah Strata 1 di Universitas Putra Indonesia “YPTK” Padang dengan jurusan Sistem Informasi. Kemudian pada tahun 2016 mendapat gelar Magister Ilmu Komputer dengan konsentrasi Sistem Informasi di Universitas Putra Indonesia “UPI YPTK” Padang. Memulai profesi sebagai Dosen pada bulan Februari 2017 hingga Juli 2024 di Universitas Pembangunan Panca Budi Medan Pada Prodi Sistem Komputer dan Program Studi Teknologi Informasi, Fakultas Sains dan Teknologi. Dan mulai pada 1 Agustus 2024, mulai aktif di Politeknik Negeri Medan menjadi seorang Dosen ASN.

Nurkhalisah

Nurkhalisah Lahir di Bireun, 1 agustus 2003. Beliau adalah mahasiswi aktif Fakultas Ilmu Sosial dan Humaniora Program Studi Ilmu Hukum Universitas Muhammadiyah Mahakarya Aceh, Bireun.

Buku *Perlindungan Hukum Tindak Pidana Cybercrime dalam Cyberlaw di Indonesia: Perkembangan Teknologi dan Tantangan Hukum dalam Mewujudkan Cybersecurity* ini membahas secara mendalam dan komprehensif berbagai aspek hukum terkait tindak pidana siber di Indonesia yang semakin krusial seiring pesatnya perkembangan teknologi informasi dan komunikasi. Di era digital yang serba terkoneksi ini, cybercrime bukan hanya menjadi ancaman bagi individu atau bisnis semata, melainkan juga bagi keamanan nasional dan ketahanan sosial ekonomi. Buku ini menguraikan fenomena cybercrime dari berbagai sudut pandang, mulai definisi dan klasifikasi jenis kejahatan siber menurut peraturan perundang-undangan nasional serta kaitannya dengan perkembangan global dalam hukum siber (cyberlaw).

Dalam buku ini dipaparkan kajian mendetail tentang kerangka hukum yang ada di Indonesia, meliputi implementasi dan evaluasi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), UU Perlindungan Data Pribadi, serta aturan lain yang mendukung penegakan hukum pada ranah siber. Bab-bab dalam buku ini mengupas pasal-pasal penting dan relevan, proses penegakan hukum, serta peran penyidik dan lembaga dalam menangani tindak pidana siber. Buku ini juga menyoroti tantangan nyata yang dihadapi oleh sistem hukum Indonesia, seperti multitafsir pada pasal-pasal tertentu, keterbatasan kapasitas penegak hukum, serta perlunya adaptasi regulasi terhadap teknologi yang terus berkembang dengan cepat. Melalui pendekatan multidisipliner, buku ini menawarkan rekomendasi dan strategi penguatan regulasi serta kebijakan yang dapat membentuk sistem cybersecurity yang lebih kuat dan responsif.

Selain dari aspek yuridis dan regulasi, buku ini juga membahas implikasi sosial dan ekonomi dari tindak pidana siber, dampaknya terhadap masyarakat dan dunia usaha, serta peran penting edukasi masyarakat dan kerjasama lintas sektor dan internasional dalam pencegahan dan penanggulangan cybercrime. Dengan bahasa yang sistematis, akademik namun tetap mudah dipahami, buku ini ditujukan bagi para akademisi, praktisi hukum, penegak hukum, pembuat kebijakan, dan masyarakat luas yang ingin mendalami aspek perlindungan hukum di ranah digital. Buku ini diharapkan dapat menjadi referensi penting dalam mengembangkan hukum siber di Indonesia serta mendorong keamanan dan kepercayaan di dunia maya.



IKAPI
INDONESIAN ASSOCIATION OF JOURNALISTS

CV. Tahta Media Group
Surakarta, Jawa Tengah
Web : www.tahtamedia.com
Ig : [tahtamedia](https://www.instagram.com/tahtamedia)
Telp/WA : +62 896-5427-3996

